CLAIMS

1. A method of managing generations of security key information in an information environment comprising a key-producing side generating and distributing key information to a key-consuming side, said method comprising the steps of:

- distributing, at key update, key information of a new key generation from the key-producing side to the key-consuming side;
- replacing, on the key-consuming side, key information of an older key generation by the key information of the new key generation;
- iteratively applying, whenever necessary, a predetermined one-way key derivation function on the key-consuming side to derive key information of at least one older key generation from the key information of the new key generation.

2. The method of claim 1, wherein the key-producing side generates the key information of said new key generation by iteratively applying an instance of the predetermined one-way key derivation function starting from key information of a predetermined generation.

3. The method of claim 2, wherein said predetermined key generation is a master key generation.

4. The method of claim 1, wherein the key-producing side generates key information of said new key generation by applying a trap-door function of the predetermined one-way key derivation function starting from key information of any older key generation.

5. The method of claim 1, wherein said step of iteratively applying a predetermined one-way key derivation function to derive key information of at least one older key generation enables the key-consuming side to use any older key

generation in the information environment even though one or more previous key updates have been missed.

6. The method of claim 1, wherein the key-producing side comprises a key-issuing server issuing security key information to be shared by: at least one communication device and a provider of protected data for said at least one communication device.

7. The method of claim 6, wherein said at least one communication device comprises a group of devices, each of which implements an instance of the predetermined one-way key derivation function, thereby enabling each group device with access to the new key generation to communicate also based on any older key generation.

8. The method of claim 7, wherein group devices with access to the new key generation are enabled to share protected data also based on any older key generation.

9. The method of claim 6, wherein the key-consuming side comprises said at least one communication device and said provider of protected data.

10. The method of claim 6, wherein said key-issuing server and said provider of protected data are integrated.

11. The method of claim 1, wherein said one-way key derivation function is implemented in a device on the key-consuming side for generating key information of said at least one older key generation from key information of the new key generation provided that additional data in the form of a predetermined access code is applied to the key derivation function.

12. The method of claim 1, wherein the key information derived by iteratively applying said one-way key derivation function directly corresponds to a cryptographic key.

13. The method of claim 1, further comprising the step of transforming said derived key information into a cryptographic key.

14. The method of claim 1, wherein said key-derivation function is based on a cryptographic hash function.

15. The method of claim 1, wherein said security key information is used for Digital Rights Management in a digital content distribution system, on-line gaming, file sharing in a Local or Personal Area Network, store-and-forward applications or for securing on-line sessions.

16. An arrangement for managing generations of security key information in an information environment having a key-producing side that generates and distributes key information to a key-consuming side, said arrangement comprising:

- means for distributing, at key update, key information of a new key generation from the key-producing side to the key-consuming side;
- means for replacing, on the key-consuming side, key information of an older key generation by the key information of the new key generation;
- means for iteratively applying, whenever necessary, a predetermined one-way key derivation function on the key-consuming side to derive key information of at least one older key generation from the key information of the new key generation.

17. The arrangement of claim 16, further comprising means for generating, on the key-producing side, the key information of said new key generation by iteratively applying an instance of the predetermined one-way key derivation function starting from key information of a predetermined key generation.

18. The arrangement of claim 17, wherein said predetermined key generation is a master key generation.

19. The arrangement of claim 16, further comprising means for generating, on the key-producing side, the key information of said new key generation by applying a trap-door function of the predetermined one-way key derivation function starting from key information of any older key generation.

20. The arrangement of claim 16, wherein said means for iteratively applying a predetermined one-way key derivation function to derive key information of at least one older key generation is operable for enabling the key-consuming side to use any older key generation in the information environment even though one or more previous key updates have been missed.

21. The arrangement of claim 16, wherein the key-producing side comprises a key-issuing server issuing security key information to be shared by: at least one communication device and a provider of protected data for said at least one communication device.

22. The arrangement of claim 21, wherein said at least one communication device comprises a group of devices, each of which comprises means for iteratively applying said one-way key derivation function, thereby enabling each group device with access to the new key generation to communicate also based on any older key generation.

23. The arrangement of claim 22, wherein group devices with access to the new key generation are enabled to share protected data also based on any older key generation.

24. The arrangement of claim 21, wherein the key-consuming side comprises said at least one communication device and said provider of protected data.

25. The arrangement of claim 21, wherein said key-issuing server and said provider of protected data are integrated.

26. The arrangement of claim 16, wherein said means for iteratively applying a one-way key derivation function is implemented in a device on the key-consuming side and configured for generating key information of said at least one older key generation from key information of the new key generation provided that additional data in the form of a predetermined access code is applied to the key derivation function.

27. The arrangement of claim 16, wherein said means for iteratively applying a one-way key derivation function is operable for deriving key information that directly corresponds to a cryptographic key.

28. The arrangement of claim 16, further comprising means for transforming said derived key information into a cryptographic key.

29. The arrangement of claim 16, wherein said key-derivation function is based on a cryptographic hash function.

30. The arrangement of claim 16, wherein said security key information is used for Digital Rights Management in a digital content distribution system, on-line gaming, file sharing in a Local or Personal Area Network, store-and-forward applications or for securing on-line sessions.

31. A security-key consuming entity in an information environment, said security-key consuming entity comprising:

- means for receiving, at key update, key information of a new key generation;
- means for replacing key information of an older key generation stored in said security-key consuming entity by the key information of the new key generation;
- means for iteratively applying, whenever necessary, a predetermined one-way key derivation function to derive key information of at least one older key generation from the key information of the new key generation.

32. A security-key producing entity in an information environment, said security-key producing entity comprising:

- means for iteratively applying a one-way key derivation function a given number of times starting from key information of a master key generation to derive key information of a predetermined key generation; and
- means for distributing a representation of the derived key information to at least one key-consuming entity in the information environment for the purpose of secure communication.
